Cisco 3251 Mobile Access Router Card FIPS 140-2 Security Policy

Level 2 Validation
Version 1.3
February 28, 2006

Introduction

This is the non-proprietary Cryptographic Module Security Policy for the Cisco 3251 Mobile Access Router Card. This security policy describes how the 3251 Mobile Access Routers Card (Hardware Version: 3.2; Firmware Version: 12.3(14)T2) meet the security requirements of FIPS 140-2, and how to operate in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Cisco 3251 Series Mobile Access Router card.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

This document contains the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

References

This document deals only with operations and capabilities of the Cisco 3251 Series Mobile Access Router card in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Cisco 3251 Series Mobile Access Router card from the following sources:

- The Cisco Systems website contains information on the full line of products at www.cisco.com. The 3200 Series product descriptions can be found at:

  http://www.cisco.com/en/US/products/hw/routers/ps272index.html
- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical or sales-related questions for the module.

Terminology

In this document, the Cisco 3251 Series Mobile Access Router cards are referred to as the Cisco 3251 router, the router, the module, or the system.

Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco 3251 Series Mobile Access Router card and explains their secure configuration and operation. This introduction section is followed by the "The Cisco 3251 Mobile Access Router Card" section on page 2, which details the general features and functionality of the router. The "Secure Operation of the Cisco 3251 Mobile Access Router" section on page 11 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

The Cisco 3251 Mobile Access Router Card

The Cisco 3251 Series Mobile Access Router cards are high-performance cards in a compact form factor ideally suited for integration in vehicles. They offer secure data, voice and video communications, seamless mobility and interoperability across multiple wireless networks.

The Cisco 3251 Series Mobile Access Router card, along with the other network interface cards (such as FESMIC and SMIC), extend the edge of the IP network to a new frontier of Networks-in-Motion and facilitates new and exciting applications in the defense, public safety, homeland security, and commercial transportation markets.

The routers offer users the following benefits:

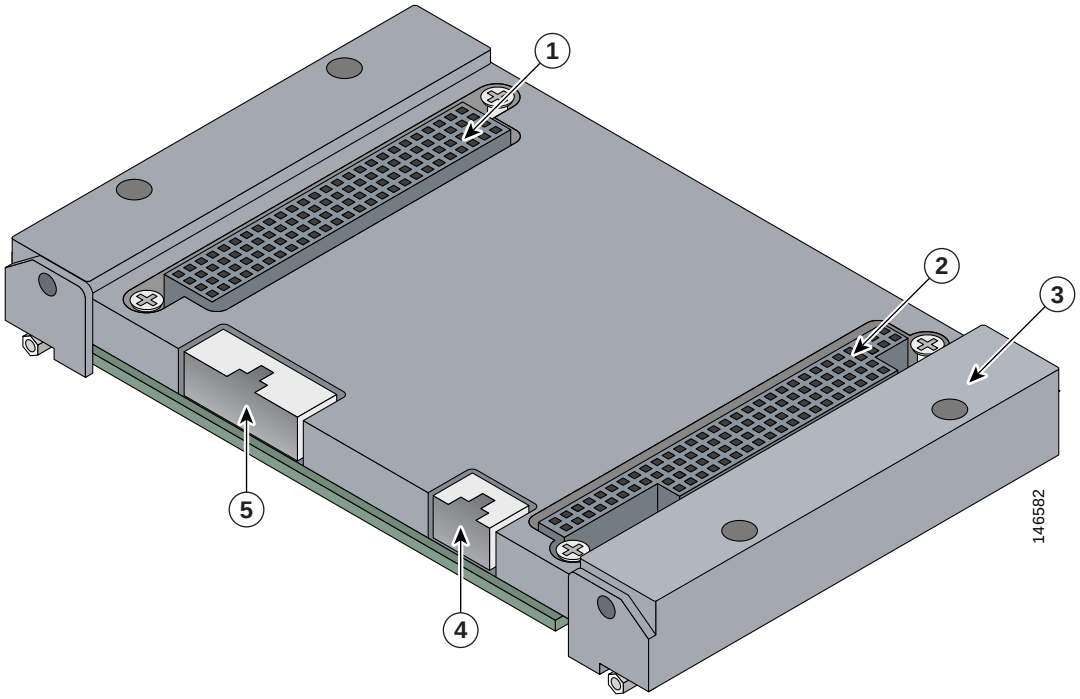
- Secure data, voice and video communications with seamless mobility across wireless networks independent of location or movement
- High performance in a compact, rugged design for use in vehicles
- Advanced IP services and interoperability through Cisco IOS Software

The Cisco 3251 Series Mobile Access Router card leverages Cisco IOS software features including Mobile Networks, security, QoS, routing and management functionality to deliver comprehensive services for Networks-in-Motion. It provides a scalable, secure, manageable router platform that meets FIPS 140-2 overall security level 2 requirements. This section describes the general features and functionality provided by the Cisco 3251 Series Mobile Access Router card.

The 3251 Cryptographic Module

Figure 1 shows the Cisco 3251 Series Mobile Access Router card layout.

Figure 1 The Bottom of the Cisco 3251 Mobile Access Router Card



1	PCI connector	**2**	ISA connector
3	Wedge Lok (one on each side of the card)	**4**	Ethernet header
5	Multifunction header		

The Cisco 3251 Series Mobile Access Router card is a multi-chip embedded cryptographic module. The cryptographic boundary is defined by the exterior surfaces of the module and the module's connectors. The connectors include the 34-pin multifunction header, the 10-pin ethernet header, the upper and lower PCI bus, and the upper and lower ISA bus. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

Module Interfaces

The Cisco 3251 routers feature a multifunctional header interface, which provides functionality to connect a console port, auxiliary ports, and system and network LEDs. The module also provides the ability to add network modules and other interface cards via the PC/104-Plus PCI interface. Network modules support a variety of serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity.

An NM is connected to the PC/104-Plus PCI bus interface. NMs interface directly with the processor, and cannot perform cryptographic functions; they only serve as a data input and data output physical interface.

The physical interfaces include an ISA interface but the card does not send or receive any data, control, or status information via the ISA interface - it provides a physical connection only (although the module will allow data used by other units to pass through the ISA bus). The PC/104-Plus PCI interface provides power to the module from the power card, as well as communications with other units. The module also has an RS-232 connector for a console terminal for local system access. The router also has a multifunctional header interface which provides status via LED pins, whose status indicators are provided in Table 1

Table 1 Cisco 3251 LED Descriptions

LED	Indication	Description
POWER	ON	Power is on
	OFF	No power
MARC (In ROMMON)		
OK	OK	OK
LINK	LINK	LINK
ACT	OFF	Normal operation
MARC (During Boot-up)		
OK	B, S	Normal operation
LINK	S, OFF, S, OFF, S	F0/0 interface is Not Shutdown and is connected to another device
	S, OFF, S	F0/0 interface is Shutdown and is connected to another device
	S, OFF	F0/0 interface is not connected to another device
ACT	OFF, S, B	F0/0 interface is Not Shutdown and is connected to another device
	OFF, S, OFF	F0/0 interface is Shutdown and is connected to another device
	OFF	F0/0 interface is not connected to another device
MARC (In IOS)		
OK	S	Normal operation
LINK	S	F0/0 interface is connected to another device

Table 1 Cisco 3251 LED Descriptions (Continued)

	OFF	F0/0 interface is not connected to another device
ACT	OFF, B	F0/0 interface is Not Shutdown and is connected to another device
	OFF	F0/0 interface is Shutdown and/or is not connected to another device

All of these physical ports are separated into the logical interfaces from FIPS 140-2 as described in Table 2:

Table 2 FIPS 140-2 Logical Interfaces

Router Physical Port	FIPS 140-2 Logical Interface
10/100 Base T Multifunctional Header PC/104-Plus PCI Interface	Data Input Interface
10/100 Base T Multifunctional Header PC/104-Plus PCI Interface	Data Output Interface
10/100 Base T Multifunctional Header PC/104-Plus PCI Interface	Control Input Interface
Multifunctional Header 10/100 Base T PC/104-Plus PCI Interface	Status Output Interface
PC/104-Plus PCI Interface	Power Interface

Roles and Services

Authentication is role-based. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. Both roles are authenticated by providing a valid password.

The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role. The module supports RADIUS and TACACS+ for

authentication and they are used in the FIPS mode. A complete description of all the management and configuration capabilities of the Cisco 3251 Series Mobile Access Router card can be found in the *Performing Basic System Management* manual and in the online help for the router.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length. See the "Secure Operation of the Cisco 3251 Mobile Access Router" section for more information. If only integers 0-9 are used without repetition for an 8 digit PIN, the probability of randomly guessing the correct sequence is 1 in 1,814,400. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

Crypto Officer Role

During initial configuration of the router, the Crypto Officer password (the **enable** password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- **Configure the router**—Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters**—Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **View Status Functions**—View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
- **Manage the router**—Log off users, shutdown or reload the outer, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass**—Set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.

User Services

Users enter the system by accessing the console port with a terminal program or via IPSec protected telnet or SSH session to a LAN port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program.

The services available to the User role consist of the following:

- **Status Functions**—View state of interfaces and protocols, version of IOS currently running.
- **Network Functions**—Connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).
- **Terminal Functions**—Adjust the terminal session (e.g., lock the terminal, adjust flow control).
- **Directory Services**—Display directory of files kept in flash memory.

Physical Security

The router must be installed within an approved chassis. Such chassis are available from various resellers; please contact your Cisco distributor for more information. Console and auxiliary port connectors are provided on the router, and the power cable connection is provided on the power supply.

Tamper evident seals are installed on the thermal plates in the factory – the Crypto Officer can determine that the module has not been tampered with by observing the integrity of the seals. There are two seals – one spans the top and bottom plate between the multifunction header and the ethernet header, and the other spans the top and bottom plate on the side opposite the first. The seals have unique serial numbers, and any attempt to remove them will leave visible evidence.

Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE).

The module supports the critical security parameters (CSPs) shown in Table 3.

Table 3 Critical Security Parameters

Name	Algorithm	Description	Storage	Zeroization Method
PRNG Seed	X9.31	This is the seed for X9.31 PRNG. This CSP is stored in DRAM and updated periodically after the generation of 400 bytes – after this it is reseeded with router-derived entropy; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this CSP.	DRAM	Automatically every 400 bytes, or turn off the router.
Diffie Hellman private exponent	DH	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated. (1536 bit modulus)	DRAM	Automatically after shared secret generated. Group 2 (1024 bit modulus) is not permitted in FIPS mode of operations. Group 5 (1536 bit modulus) is the only DH group permitted.
Diffie Hellman public exponent	DH	The public exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated. (1536 bit modulus)	DRAM	Automatically after shared secret generated. Group 2 (1024 bit modulus) is not permitted in FIPS mode of operations. Group 5 (1536 bit modulus) is the only DH group permitted.
skeyid	Keyed SHA-1	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM	Automatically after IKE session terminated.
skeyid_d	Keyed SHA-1	The IKE key derivation key for non ISAKMP security associations.	DRAM	Automatically after IKE session terminated.

Table 3 Critical Security Parameters (Continued)

skeyid_a	SHA-1 HMAC	The ISAKMP security association authentication key.	DRAM	Automatically after IKE session terminated.
skeyid_e	TDES/AES	The ISAKMP security association encryption key.	DRAM	Automatically after IKE session terminated.
IKE session encrypt key	TDES/AES	The IKE session encrypt key.	DRAM	Automatically after IKE session terminated.
IKE session authentication key	SHA-1 HMAC	The IKE session authentication key.	DRAM	Automatically after IKE session terminated.
ISAKMP preshared	Secret	The key used to generate IKE skeyid during preshared-key authentication. “no crypto isakmp key” command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM	“# no crypto isakmp key”
IKE hash key	SHA-1 HMAC	This key generates the IKE shared secret keys. This key is zeroized after generating those keys.	DRAM	
secret_1_0_0		The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash memory.	NVRAM	
IPSec encryption key	TDES/AES	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM	Automatically when IPSec session terminated.
IPSec authentication key	SHA-1 HMAC	The IPSec authentication key. The zeroization is the same as above.	DRAM	Automatically when IPSec session terminated.
Configuration encryption key	AES	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued. Note that this command does **not** decrypt the configuration file, so zeroize with care.	NVRAM	“# no key config-key”
Router authentication key 1	Shared secret	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM	Automatically upon completion of authentication attempt.
PPP authentication key	RFC 1334	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM	Turn off the router.
Router authentication key 2	Shared Secret	This key is used by the router to authenticate itself to the peer. The key is identical to Router authentication key 1 except that it is retrieved from the local database (on the router itself). Issuing the “no username password” zeroizes the password (that is used as this key) from the local database.	NVRAM	“# no username password”

Table 3 Critical Security Parameters (Continued)

SSH session key	Various symmetric	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM	Automatically when SSH session terminated
User password	Shared Secret	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
Enable password	Shared Secret	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
Enable secret	Shared Secret	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
RADIUS secret	Shared Secret	The RADIUS shared secret. This shared secret is zeroized by executing the “no radius-server key” command.	NVRAM DRAM	“# no radius-server key”
TACACS+ secret	Shared Secret	The TACACS+ shared secret. This shared secret is zeroized by executing the “no tacacs-server key” command.	NVRAM DRAM	“# no tacacs-server key”
Mobile authentication key	HMAC MD5	A shared secret key for authentication to other mobile agents	NVRAM	“# no ip mobile secure home-agent” “# no ip mobile secure foreign-agent” “# no ip mobile secure host”

Note All RSA operations are prohibited by policy, and commands that can be executed by Officer are shown “# command”.

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in the Table 4.

Table 4 Role and Service Access to CSP

SRDI/Role/ Service Access Policy	Security Relevant Data Item	PRNG Seed	DH private exponent	DH public exponent	skeyid	skeyid_d	skeyid_a	skeyid_e	IKE session encrypt key	IKE session authentication key	ISAKMP preshared	IKE hash key	secret_1_0_0	IPSec encryption key	IPSec encryption key	SSL session key	Configuration encryption key	Router authentication key	PPP Authentication key	Router authentication key 2	SSH session key	User password	Enable password	Enable secret	RADIUS secret	TACACS+ secret	Mobile Authentication Key
Role/Service																											
User Role																											
Status Functions																											
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r		r	r	r	r	r					r
Crypto-Officer Role																											
Configure the Router													r w d				r w d			r w d							r w d
Manage the Router		d															r w d	r w d	d			r w d	r w d	r w d	r w d	r w d	r w d
Set Encryption/ Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d	r w d			r w		r w d						

The module supports the following FIPS approved algorithms: 3DES, AES, SHA-1, HMAC SHA-1, and X9.31 PRNG. It also supports the following non-approved algorithms: DES, MD5, HMAC MD5, Diffie-Hellman, RSA. The DES, MD5, HMAC MD5, and RSA algorithms shall not be used in FIPS mode. Diffie-Hellman is allowed for use in key establishment.

The module supports two types of key management schemes:

1. Pre-shared key exchange via electronic key entry. 3DES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.
2. Internet Key Exchange method with support for pre-shared keys exchanged and entered electronically.
   - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive 3DES or AES keys.
   - The pre-shared key is also used to derive HMAC-SHA-1 key.

The module supports commercially available methods of key establishment, including Diffie-Hellman and IKE.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol.

Key Zeroization

All of the keys and CSPs of the module can be zeroized. Please refer to the *Description* column of Table 3 for information on methods to zeroize each key and CSP.

Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. If any of the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Power-up Tests

- Firmware integrity test
- AES KAT
- DES KAT
- TDES KAT
- SHA-1 KAT
- PRNG KAT
- Power-up bypass test
- Diffie-Hellman self-test
- HMAC SHA-1 KAT

Conditional Tests

- Conditional bypass test
- Continuous random number generator tests

Secure Operation of the Cisco 3251 Mobile Access Router

Cisco 3251 Series Mobile Access Router cards meet all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

Initial Setup

The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal
no service password-recovery
end
show version
```

Note Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 12.3(14)T2, Advanced Security build (advsecurity) is the only allowable image; no other image may be loaded.
2. The value of the boot field must be 0x0101. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the *configure terminal* command line, the Crypto Officer enters the following syntax:

   ```
   config-register 0x0101
   ```

3. The Crypto Officer must create the **enable** password for the Crypto Officer role. The password must be at least 8 characters to include at least one number and one letter and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the # prompt:

   ```
   enable secret [PASSWORD]
   ```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the *configure terminal* command line, the Crypto Officer enters the following syntax:

   ```
   line con 0
   password [PASSWORD]
   login local
   ```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).
6. The Crypto Officer shall not assign a command to any privilege level other than its default.
7. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
8. If the Crypto Officer loads any IOS image onto the router, this will put the router into a non-FIPS mode of operation.

IPSec Requirements and Cryptographic Algorithms

1. The only type of key management protocol that is allowed in FIPS mode is Internet Key Exchange (IKE), although manual creation of security associations is also permitted.

2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:
   - ah-sha-hmac
   - esp-sha-hmac
   - esp-3des
   - esp-aes
3. The Crypto Officer shall configure the module to use Diffie-Hellman group 5 by using the following commands:

   Router(config)#**crypto isakmp policy** *10*

   Router(config-isakmp)#**group** *5*

Using the Diffie-Hellman groups implemented by the module, the effective symmetric key strength is 80 to 96 bits.

4. The following algorithms are not FIPS-approved and shall not be used during FIPS-approved mode:
   - MD-5
   - MD-5 HMAC
   - RSA (may not be used either for key transport or digital signatures)
   - DES

Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP gets and sets. Since SNMP v2C uses community strings for authentication, all SNMP v2C operations must be performed within a secure IPSec tunnel between the remote system and the module.

Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.
2. SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

Related Documentation

For more information about the Cisco 3251 Series Mobile Access Router card, refer to the following documents:

- *Cisco 3200 Series Router Hardware* documents
- *Cisco 3200 Series Router Software Configuration* documents

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- Non-emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by Cisco Systems.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.